UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,371	10/05/2001	Ryuichi Iwamura	SONY-50R4813	4728

7590 09/01/2006

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/972,371	**Applicant(s)** IWAMURA, RYUICHI	
	Examiner Benjamin E. Lanier	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 17-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 17-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 October 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 17 July 2006 has been entered.

Response to Arguments

2. Applicant's arguments filed 17 July 2006 have been fully considered but they are not persuasive. Applicant's argument allegation that Deo discloses global secrets is not persuasive because Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). A private key is not a global secret because it is private. It is the smart card in Deo that stores the digital certificate, not the set top box. Therefore, applicant's allegation that Spies teaches away from the system disclosed on Deo is not persuasive because although Spies mentions that the preferred embodiment of the hardware not store global secrets, MPEP 2123 states:

> PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN
>
> "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)).

> **A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments.** Merck & Co. v.Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention. "The fact that a modem with a single carrier data signal is shown to be less than optimal does not vitiate the fact that it is disclosed.").
>
> NONPREFERRED AND ALTERNATIVE EMBODIMENTS
> CONSTITUTE PRIOR ART
>
> Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994) (The invention was directed to an epoxy impregnated fiber-reinforced printed circuit material. The applied prior art reference taught a printed circuit material similar to that of the claims but impregnated with polyester-imide resin instead of epoxy. The reference, however, disclosed that epoxy was known for this use, but that epoxy impregnated circuit boards have "relatively acceptable dimensional stability" and "some degree of flexibility," but are inferior to circuit boards impregnated with polyester-imide resins. The court upheld the rejection concluding that applicant's argument that the reference teaches away from using epoxy was insufficient to overcome the rejection since "Gurley asserted no discovery beyond what was known in the art." 27 F.3d at 554, 31 USPQ2d at 1132.). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed…." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004).

3. Therefore, it would have been obvious to one of ordinary skill in the art would have been at the time the invention was made to include the public key of the set top box of Spies, and encrypt the decryption key using the public key of the set top box so that the encryption key can only be decrypted using the private key of that particular set top box, and no other set top box (Deo: Col. 2, lines 45-47).

4. Applicant's argument that the prior art fails to teach of fairly suggest the limitation "at said first logical circuit, decrypting said encrypted signal using said first decryption key," is not

persuasive because Spies discloses Encrypted video data is received at the set top box (Figure 7) and passed to the processor of the set top box, along with the decryption key from the IC card, to facilitate decryption of the video data (Col. 12, line 61 – Col. 13, line 10). The set top box processor (Figure 7, element 150), meets the limitation of the recited "first logical unit". Careful review of Figure 7 and Col. 12, line 61 – Col. 13, line 10, of Spies shows that the set top box (Figure 7, element 60) decrypts the encrypted video signal using a decryption routine (Figure 7, element 162) that is executed on the set top box processor (Figure 7, element 150).

5. Applicant's argument that Spies does not disclose "replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program", because "Spies teaches such CSPs are preferably...stored in ROM (read only memory)...cannot be replace as recited by Claim 4," is not persuasive because the CSPs referred to by Applicant are cryptographic service providers (Col. 11, line 52). The elements relied upon in Spies are actually the **cryptographic functions** (Col. 12, line 2), which Spies specifically states are updated by **replacing** one or more DLLs (Col. 12, lines 1-4). Therefore, the aforementioned limitation from claim 4, is anticipated by Spies.

6. Applicant has requested art to support the fact that satellite television and DVDs utilize the MPEG-2 format. The MPEG Handbook (See Attachment) states that, "Digital television broadcasting relies on the combination of a number of fundamental technologies. These are: **MPEG-2 compression to reduce the bit rate**, multiplexing to combine picture and sound data into a common bitstream, digital modulation schemes to reduce the RF bandwidth needed by a given bit rate and error correction to reduce the error statistics of the channel down to a value acceptable to **MPEG data** (Pages 368-369)." Therefore, not only does satellite television utilize

MPEG-2 format, but every digital television broadcasting service utilizes MPEG-2 format. The MPEG Handbook goes on to say, "The greatly increased capacity of DVD means that moderate compression factors can be employed. **MPEG-2 coding is used**, so that progressively scanned or interlaced material can be handled (Page 390)." Therefore, Spies recitation of the video signal coming from satellite television networks or DVDs, meets the limitation of the video signal being compliant with the MPEG format.

7. Applicant alleges that one of the local memories in the set top box of Spies is in fact observable, but has not provided any evidence in the Spies reference to support his allegation.

8. Applicant's argument that the packet keys are never made available to the set top box of Spies is not persuasive because (Col. 12, line 61 – Col. 13, line 10) of Spies shows that the individual packet keys are used by the IC card to generate the decryption keys that are used by the processor of the set top box to decrypt the encrypted video signals using the stored decryption routine.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnston, U.S. Patent No. 6,373,946. Referring to claim 17, Johnston discloses a communication security system wherein a mobile handset terminal (Figure 2) comprises a terminal processor (Figure 2,

element 37) and a SIM card (Figure 2, element 35). The mobile handset terminal meets the limitation of the digital media receiving device. The SIM card meets the limitation of a first logical circuit, and the terminal processor meets the limitation of the second logical circuit. The SIM card receives a partial key that is used to generate an encryption key (Col. 10, lines 36-43, 52-53 & Col. 11, lines 14-17). The SIM card supplies this encryption key to the terminal processor to encrypt data (Col. 10, lines 51-53), which meets the limitation of a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit. Prior to transmitting the encryption key to the terminal processor, the SIM card decrypts the partial key that is ultimately used to generate the encryption key (Col. 12, lines 20-24), which meets the limitation of a first logical circuit for decrypting a local encryption key. The SIM card contains a processor (Figure 2, element 35a) and a memory (Figure 2, element 35b & Col. 6, lines 20-23), which meets the limitation of said first logical circuit comprising a local processor and local memory.

Referring to claim 18, Johnston discloses that the SIM card stores an encryption algorithm to decrypt data (Col. 12, lines 8-12), which meets the limitation of a computer control program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical circuit.

Referring to claim 19, Johnston discloses that the SIM cards are reprogrammable so that they may be tailored so specific communication environments (Col. 16, lines 47-49), which meets the limitation of a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory.

Referring to claim 20, Johnston discloses that the data stored in the SIM cannot be read or accessed (Col. 1, lines 36-37), which meets the limitation of the contents of said local memory cannot be observed from outside of said first logical circuit.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claims 1, 3-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781. Referring to claim 1, Spies discloses a secure video content delivery system wherein an IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of generating a public encryption key. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55).

Encrypted video data is received at the set top box (Figure 7) and passed to the processor of the set top box, along with the decryption key from the IC card, to facilitate decryption of the video data (Col. 12, line 61 – Col. 13, line 10), which meets the limitation of in a digital media receiving device, accessing an encrypted signal at said first logical circuit, determining a first decryption key for said encrypted signal at said logical circuit, at said first logical circuit decrypting said encrypted signal using said first decryption key. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 3, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55), which meets the limitation of accessing a computer control program for a second portion of local of local memory at said second logical circuit. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claims 4, 5, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). The IC card functionality can be updated or changed (Col. 12, lines 1-4), which meets the limitation of replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 6, Spies discloses that the cryptographic functions can be updated by replacing DLLs (Col. 12, lines 1-4), which meets the limitation of accessing a second decryption key from a first portion of local memory at said first logical circuit, replacing a computer control program stored in a second portion of local memory at least first logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory, and executing said new computer control program at said second logical circuit to decrypt said first decryption key using said second decryption key.

Referring to claim 7, Spies discloses that the video content can be TV broadcasts (Col. 1, lines 14-29), which are transmitted in MPEG format.

14. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781 as applied to claim 1 above, and further in view of Schneier. Referring to claim 2, Spies does not disclose using Diffie-Hellman algorithm for key exchange. Schneier discloses using the Diffie-Hellman algorithm for public key exchange (Pages 513-514). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the Diffie-Hellman algorithm for public key exchange in

the secure video content delivery system of Spies because Diffie-Hellman gets its security from the difficulty of calculating discrete logarithms in a finite field as taught by Schneier (Page 513).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier